AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions of claims in the application. Claims 1, 17 and 33 have been amended herein.

1. (Currently amended) A method of controlling at a gateway computing device access of a client machine to a desired resource hosted on a destination server, the desired resource being of at least one material type selected from the group including audible materials, readable materials, and viewable materials, comprising ~~the steps of~~:

~~(a)~~ at the gateway computing device receiving handshaking packets from the client machine having as a destination address the destination server;

~~(b)~~ redirecting network communications at the gateway computing device, including ~~the steps of~~:

redirecting the entirety of each of the handshaking packets by rewriting the destination address in the handshaking packets' IP headers to route the packets to an access controlling web server that is remote from the client, the gateway, and the destination server;

receiving a content request packet from the client machine at the gateway destined for the destination server intended to retrieve the desired resource from the destination server; and

at the gateway redirecting the content request packet in its entirety by rewriting the destination address in the packet IP header to route the packet to the access controlling web server;

~~(c)~~ receiving a response at the gateway from the access controlling web server; and

~~(d)~~ at the gateway, controlling access of the client machine to the desired resource based on the response from the access controlling web server, including refusing the client machine access to the desired resource if the response from the access controlling web server indicates that the client should not have access to the desired resource and granting the client machine access to the desired resource if the response from the access controlling web server indicates that the client should have access to the desired resource.

2. (Original) The method according to claim 1, wherein the step of controlling access to the desired resource based on the response from the access controlling web server further comprises the step of:

establishing a connection between the client machine and the destination server if the response indicates that access to the desired resource is allowable.

3. (Original) The method according to claim 2, wherein the content request packet comprises a GET URL packet.

4. (Original) The method according to claim 3, wherein the response indicates that access to the desired resource is allowable if the access controlling web server does not recognize the URL of the GET URL packet.

5. (Original) The method according to claim 4, further comprising the step of refusing a connection to the destination server, and establishing instead a connection between the client machine and the access controlling web server if the response is that the access controlling web server recognizes the URL of the GET URL packet.

6. (Original) The method according to claim 5, wherein the step of establishing a connection between the client machine and the destination server comprises: resending the handshaking packets and GET URL packet to the destination server transparently with respect to the client machine.

7. (Original) The method according to claim 6, further comprising the step of embedding an identity token readable by the access controlling web server in the GET URL packet, wherein the identity token uniquely identifies the client machine.

8. (Original) The method according to claim 6, further comprising the step of determining whether to redirect network communications based on the content of a handshaking packet.

9. (Original) The method according to claim 8, wherein the step of determining whether to redirect network communications comprises deciding to redirect network communications if the handshaking packet is a SYN packet directed to port 80 on the destination server.

10. (Original) The method according to claim 3, wherein the response indicates that access to the desired resource is allowable if the access controlling web server recognizes the URL of the GET URL packet.

11. (Original) The method according to claim 10, further comprising the step of refusing a connection to the destination server, and establishing instead a connection between the client machine and the access controlling web server if the response indicates that the access controlling web server does not recognize the URL of the GET URL packet.

12. (Original) The method according to claim 11, wherein the access controlling web server is an RSACi Web Server.

13. (Original) The method according to claim 11, wherein the step of establishing a connection between the client machine and the destination server comprises: resending the handshaking packets and GET URL packet to the destination server transparently with respect to the client machine.

14. (Original) The method according to claim 13, further comprising the step of embedding an identity token readable by the access controlling web server in the GET URL packet, wherein the identity token uniquely identifies the client machine.

15. (Original) The method according to claim 13, further comprising the step of determining whether to redirect network communications based on the content of a handshaking packet.

16. (Original) The method according to claim 15, wherein the step of determining whether to redirect network communications comprises deciding to redirect network communications if the handshaking packet is a SYN packet directed to port 80 on the destination server.

17. (Currently amended) A computer-readable medium having computer-executable instructions for controlling access at a gateway computer of a client to a desired resource hosted on a destination server comprising ~~the steps of~~:

~~(a)~~ receiving handshaking packets at the gateway computer from the client machine having as a destination address an address corresponding to the destination server;

~~(b)~~ redirecting network communications at the gateway computer, including ~~the steps of~~:

redirecting the handshaking packets in their entirety by rewriting the destination address in the handshaking packets' IP headers to route the packets to an access controlling web server that is remote from the gateway computer;

receiving a content request packet from the client machine destined for the destination server intended to retrieve the desired resource from the destination server; and

redirecting the entirety of the content request packet by rewriting the destination address in the packet IP header to route the packet to the access controlling web server;

~~(c)~~ receiving a response at the gateway computer from the access controlling web server; and

~~(d)~~ at the gateway computer controlling access of the client machine to the desired resource based on the response from the access controlling web server by granting access if the response indicates that the client may access the desired resource and denying access if the response indicates that the client may not access the desired resource.

18. (Original) The computer-readable medium of claim 17, wherein the step of controlling access to the desired resource based on the response from the access controlling web server further comprises the step of:

establishing a connection between the client machine and the destination server if the response indicates that access to the desired resource is allowable.

19. (Original) The computer-readable medium of claim 18, wherein the content request packet comprises a GET URL packet.

20. (Original) The computer-readable medium of claim 19, wherein the response indicates that access to the desired resource is allowable if the access controlling web server does not recognize the URL of the GET URL packet.

21. (Original) The computer-readable medium of claim 20, further comprising the step of refusing a connection to the destination server, and establishing instead a connection between the client machine and the access controlling web server if the response is that the access controlling web server recognizes the URL of the GET URL packet.

22. (Original) The computer-readable medium of claim 19, wherein the step of establishing a connection between the client machine and the destination server comprises: resending the handshaking packets and GET URL packet to the destination server transparently with respect to the client machine.

23. (Original) The computer-readable medium of claim 22, further comprising the step of embedding an identity token readable by the access controlling web server in the GET URL packet, wherein the identity token uniquely identifies the client machine.

24. (Original) The computer-readable medium of claim 22, further comprising the step of determining whether to redirect network communications based on the content of a handshaking packet.

25. (Original) The computer-readable medium of claim 24, wherein the step of determining whether to redirect network communications comprises deciding to redirect network communications if the handshaking packet is a SYN packet directed to port 80 on the destination server.

26. (Original) The computer-readable medium of claim 19, wherein the response indicates that access to the desired resource is allowable if the access controlling web server recognizes the URL of the GET URL packet.

27. (Original) The computer-readable medium of claim 26, further comprising the step of refusing a connection to the destination server, and establishing instead a connection between the client machine and the access controlling web server if the response indicates that the access controlling web server does not recognize the URL of the GET URL packet.

28. (Original) The computer-readable medium of claim 27, wherein the access controlling web server is an RSACi Web Server.

29. (Original) The computer-readable medium of claim 27, wherein the step of establishing a connection between the client machine and the destination server comprises: resending the handshaking packets and GET URL packet to the destination server transparently with respect to the client machine.

30. (Original) The computer-readable medium of claim 29, further comprising the step of embedding an identity token readable by the access controlling web server in the GET URL packet, wherein the identity token uniquely identifies the client machine.

31. (Original) The computer-readable medium of claim 29, further comprising the step of determining whether to redirect network communications based on the content of a handshaking packet.

32. (Original) The computer-readable medium of claim 31, wherein the step of determining whether to redirect network communications comprises deciding to redirect network communications if the handshaking packet is a SYN packet directed to port 80 on the destination server.

33. (Currently amended) In a computer network environment comprising a client, a hosting server, an access controlling server, and a gateway interposed between the client and both of the hosting server and the access controlling server, a method of controlling access of the client to a desired resource hosted on the hosting server, comprising ~~the steps of~~:

~~(a)~~ receiving at the gateway a request packet from the client for the desired resource and redirecting the entire request packet to the access controlling server;

~~(b)~~ receiving at the gateway a permission notification from the access controlling server in response to the redirected request packet; and

~~(c)~~ choosing to either grant or deny access of the client machine to the desired resource based on at least one criterion including the content of the permission notification received from the access controlling server.